Windows とウイルスの話

経済学部　藤田 渉

平成6年（1994年）4月に経済学部の情報化推進委員に任命され、また同時に全学のネットワーク調整委員（現NUNet運用専門委員）を引き継いだことから、平成10年4月に経済学部の部局 LAN の管理と教育用情報処理設備の運用管理を公式に担当する情報化推進室が新設されるまでの4年間にわたり、経済学部PC室の導入から運用管理まで深く関わることになった。この期間に軽微ではあったもののコンピュータ・ウイルス（以下、ウイルスと略記）の感染にも直面し、また学部としての防護対策を立案するなどの経験を持った。もとよりウイルスやその駆除方法について幅広い知見・ノウハウを持つわけではない。単に部局としての対応という、どちらかと言えば貴重な体験ができただけであり、それを通して得た雑感などを紹介させていただく。

（1）　Windows系のPCにおけるウィルスの概観

従来は感染プラットフォーム別のウィルス分類というものがあり、(1) DOS ウイルス、(2)MAC ウイルス、(3) UNIX ウイルス等に分類されてきた。これはアーキテクチャが異なるため、異なるプラットフォーム用に設計されたウィルスは、これ自体はプログラムなので感染できないしまた実行できなかったためである。全世界的な普及台数から見ても、プログラマの数から見ても(1)のDOSウィルスが圧倒的に多いとされる。

Windows 系（3.x、WFW、95/98、NT、および OS/2）のウィルスを考えるには、その主たるプラットフォームである PC/AT 互換機（およびそれらの類縁である i86PC 群、PC-9800 系など）と、その本来の OS である MS-DOS（PC-DOS）における(1)の DOS ウィルスから見て行く必要があるだろう。その理由は現在Windows系のOSを採用するPCのほとんどはこのPC/AT互換機であり、Windows 系で問題となるウィルスの多くもこのアーキテクチャおよび元来は一体化していた OS である DOS を対象に作られてきたためである。さらに現在は Windows 系と言うべきか、市場占有率の高い Microsoft 社製のマルチプラットフォーム・アプリケーションを悪用するウィルスが出現してきており、PC 自体が Intel 基準から Microsoft 基準に変容してきたことに軌を一にする様相になっている。たとえばマクロ・ウィルスのように MS-Word や MS-Excel といったマルチプラットフォームのアプリケーションで用いられるドキュメントに感染するようなタイプや Web ブラウザでダウンロードされ実行されるアクティブ・コンテンツ（ActiveX など）に組み込まれたものといった「マルチプラットフォーム」でのウィルスや不正コードが出現し、社会問題化したことでもそれがうかがわれるだろう。このようにPC/AT互換機あるいは DOS/Windows 系のプラットフォーム概念には揺らぎが生じているが、ワクチンソフトのマニュアルを含め、「DOS ウイルス」という記述でまだ統一されているようである。

現在、純粋な DOS 環境での PC は激減したと考えられるが、DOS のシェルに近く DOS に多くの機能を依存している Windows3.1 や、DOS 互換モードを持つ上に内部に DOS との共通部の多い Windows95（98 もその設計を引きずっている）では依然これらの DOS ウィルスの脅威下にある。またわが国でも PC/AT 互換機が主流になってきたために、世界標準的な（？）ウィルスに感染する可能性がさらに高まったこともこの脅威に輪をかけることになっている（IPA への日本におけるウイルスの被害届出には 1994 年 3 月と、1997 年 7 月を中心の 2 つの山があり、1994 年は国外で作成された DOS ウイルスが日本に上陸したことが原因とされ、後

者の山はマクロ・ウィルスと考えられる)。

Windows 系では DOS 環境よりもメモリ管理が厳しくなったことやブラックボックス化された DLL を用いることにより伝統的な DOS ウィルスの多くは機能しなくなったと言われたが、感染は可能なものが非常に多く、感染すれば 16 ビット互換環境（DOS 互換モード、DOS 窓、DOS セッションなど）では通常のウィルスとして動作し、さらに予定外の動作として 32 ビット実行ファイルに 16 ビットコードを書き込みダメージを与えたり、WindowsNT の NTFS に FAT 情報を書き込んでファイルシステムを破壊したりすることになる。また論理ディスクのブートセクタや、ハードディスク（HDD）のマスターブートレコード（MBR)、パーティションテーブルといったシステム領域に感染・侵入する場合も起動不能も含めて多くの誤動作を生じさせることになる（OS/2 でも類似のことが生じる)。本来、伝統的な DOS ウィルスは PC ユーザにその感染動作を秘匿することが多いが、Windows 環境では意図しない破壊により PC を機能不全にするということで発見されることになるのは皮肉なことではある。以前は感染するのみでとりたてて被害が無い（HDD やメモリを少々占有して本来ユーザが利用できる資源をわずかばかり圧迫したという程度）ということで良性のウィルスという考え方があり、悪性か良性かという分類があったことがある。しかしながら本来意図したウィルスの動作ではなく、意図しなかった悪影響も生じうるという点では、この分類はもはや考慮する必要はないであろう。

従って Windows 系の PC においても依然、旧態の DOS ウィルスから最新のウィルスまで連続して注意をはらう必要がある（Windows「専用」のウィルスはわずかしか無いようである)。またネットワーク PC（モデムや LAN に接続された PC）が普遍化したことやマルチプラットフォーム環境の進展により、その全容を常に把握・理解することは一般に容易でなくなってきている。さらに注意すべき点としてコンピュータウィルスという用語自体が記号化し、ことさらに生物学的な「ウィルス」との連想から神経質や懐疑的になり、デマウィルスなどの跳梁を許すことにもなることがあげられる。

（2）DOS/Windows 系ウィルスの分類

ウィルスの分類は、どのような症状を引き起こすかという興味本意で見られがちであるが、感染経路の遮断や駆除といったセキュリティの立場からは、その形態や機能、また感染場所・方法による分類をまず理解しておく必要があるだろう。

有名な Frederick B. Cohen の定義（1984）によればそれはプログラムであり、他のプログラムに寄生して自己増殖（自己複製＝感染（PC 内部）・伝染（他の PC））することになるので、まずそれが独立したプログラムなのか宿主のプログラムを必要とするのか、また単なるトリガイベント（論理的なきっかけで実行されること）するのか自己増殖もするのか、という点でウィルスと他の不正プログラム類と区別した分類が可能である。通産省のコンピュータウイルス対策基準によれば自己伝染機能、潜伏機能、発病機能の一つ以上有するものとされる。ウィルスは自己増殖の機能と共に通常トリガイベントも持つことが多い。

○不正プログラム一般とウィルスの区別（DOS/Windows 系）

ウィルスは不正プログラムの特徴であるトリガイベントによる発病（潜伏と発病、発病については意図したものと意図しなかったものまで含める）と同時に自己複製機能、および宿主プログラムに対する寄生を特徴とするものとして定義される。下表中、網掛けの部分が DOS/Windows 系での広義のウィルスに相当する。

		独立性		トリガイベント				Multi-Platform	
		偽装	寄生	トロイの木馬	論理爆弾	時限爆弾	瞬時爆弾		
不正なProgram	自己複製しない	○	-	○	○	○	-	-	広義のトロイの木馬
		○	△	△	△	△	○	○	不正なアクティブコンテンツなど
		○	-	○	○	○	-	-	ワーム・バクテリア
	自己複製する	-	○	○	○	○	-	-	狭義のウィルス
不正な非Program		-	○	○	○	○	-	○	マクロウィルスなど

ここでトリガイベントの種類は潜伏・発病の形態の相違に相当し、大別すれば以下のようになる。

- （狭義の）トロイの木馬（Trojan house）：一見有用なプログラム中に隠蔽、実行と同時に発病
- 論理爆弾（Logic bomb）：特定条件で発病のトリガ(Logic Trigger)がかかる
- 時限爆弾（Time bomb）：特定の時刻で発病のトリガ(Time Trigger)がかかる。
- （日時に関して論理トリガがかかるという点では論理爆弾の一種といえる）
- 瞬発爆弾（Instantaneous bomb）：侵入・ダウンロード即発病

「プログラムである」という定義は若干拡張しておく必要があるだろう。これは前述のようにMS-Wordや MS-Excel 等で作成したデータファイルに感染し、アプリケーションの正規の実行を悪用する、いわゆるマクロウィルスなどが出現しているからである。

ウィルス以外の不正プログラム（悪意のあるプログラム、被害を及ぼすプログラム）にはよく知られたトロイの木馬があるが、これは広義には一見有用なプログラム中に隠蔽してあり、実行と同時に、あるいはトリガイベントにより発病（不正なコードが実行され、正常なコンピュータ機能を阻害）するようなプログラムの総称でもある。有用なプログラム中に隠蔽ということで一見独立した不正プログラムではないように見えるが、不正コードを隠蔽したプログラム自体を独立した不正プログラムと考えるためであり、ウィルスの定義では独立したプログラムかどうかという定義は寄生先の宿主プログラムが必要かどうかということが重要である。

また自己複製機能を持つという特徴を持つだけならばウィルス以外にもワーム（Worm）とかコンピュータ・バクテリアと呼称される他のプログラムの力を借りず単独で増殖できる、独立した不正なプログラムが存在する。特にワームはUNIX時代からネットワークを介して不正なタスクをコピーして増殖するものを指す。ウィルスとはこれらと異なり感染・実行には他のプログラム（宿主プログラム）を必要とするものを指す。

以上は古典的なウィルスと他の不正プログラムとの区別に関することであるが、さらにいくつかの最近の問題点を指摘しておこう。ウィルスも含めて従来型の不正プログラムでは潜伏・発病というプロセスを持ち、トリガがかかるまでの期間に対処が可能であった。いずれも入手（侵入）してから発病するまでの期間に事前チェックや隔離されたマシン上での確認が可能である。また入手経路（感染経路）自体がFDやFTPサイトや商用PCネットからのダウンロードのような古典的なメディアを介することが多かった。しかし大衆ネットワーク時代においては、ネットワークからダウンロードで即発病という可能性のある瞬発爆弾の脅威が指摘されるようになってきている。たとえばActiveXは分散コンポーネント・オブジェクト・モデル（DCOM：Distribute Component Object Model）技術を用いたネットワーク対応の利便性を追求したコンポーネントであり Web ブラウザを介して実行されるものであるが、基本的になんで

も可能（外部からも含め）の手段を提供するとされている。これは Web や FTP サイトからのダウンロードとは異質なものであり、ダウンロード即実行であり事前チェックや隔離されたマシン上での確認といった従来の方法が使えない。現状では電子署名の情報を付加して実行前にユーザが判断をするという方法がとられているが、電子署名は作成者の認証でありプログラム自体の安全性を保証するものではないこと、またデジタルデータである電子署名は常に改竄の脅威下にあるため、多少の安全性向上でしかないといわれている。

ActiveX に比較して元来ネットワークを前提に開発された Java は JavaVM 下で機能制限が課せられ安全性が高いとされている。しかしこれも悪意ある技術とのいたちごっこであり将来はどのようなセキュリティホールがアタックされるかは分からない。現在、ネットワーク PC 上の操作は Web ブラウザが中心であり、またデスクトップは Web ブラウザとの統合化が進んでいる。コンピュータやネットワークの大衆化は市場戦略上利便性の追求がなされるが、ブラックボックスの普及は逆に絶好の攻撃対象になるわけで、今後の動向には目が離せない。この意味で、ウィルスのみを PC のセキュリティで注目するのはやや時代遅れかもしれない。

また直接ウィルスの定義に関係はないが、ユーザが形式的には自分で取り込んだもののその機能を察知していないプログラムについて、不正か不正でないかの線引き問題が残存していることは興味深い。たとえばネットワーク時代においてはサービス提供側にもユーザにもメリットがあるということで納得ずくでユーザ PC に置かれるブラックボックスのプログラムを「エージェント」と呼称するが、個人情報収集などの面でいろいろトラブルが起こるようである。これはネットワーク上やデジタル社会のプライバシーについては社会通念や私権の範囲が確定していないためである

実はこの問題はウィルスを含め不正プログラムの概念をさらに複雑にしていく議論である可能性がある。なぜならウィルスなど最初から「悪意」を意図してプログラミングされたものは明瞭であるが、「とりたてて悪意でない」意図のプログラムでも、どの時点で未確定の「私権」を侵犯する可能性があるかという「未必の故意」の議論に繋がるからである。「不正」の概念は拡大する可能性を秘めているといえよう。

○感染経路・感染場所による分類

独立した不正プログラムとの相違は、感染の方法および感染場所に関して顕著である。伝統的な DOS ウィルスにおいては感染経路で大きく 2 種類のウィルスに大別されてきた。それはいずれもプログラムであり、「実行可能プログラムファイル感染型」と「システム領域感染型（代表的なものはブートセクタ感染型）」である。FD など伝統的なメディアを介在して感染してきた時期にはシステム領域感染型の被害が多かったが、今後はネットワークを介在することにより実行可能プログラムファイル感染型の被害が増加すると考えられる。

（A）実行可能プログラムファイル感染型：

特徴としてはウィルス単体ではプログラムの実行・複製はできず、実行可能ファイルに付着・置換することで制御を奪う必要がある。多くは.COM や.EXE ファイルを付着対象（または置換対象）とするが、さらに.SYS、.DRV、.BIN、.OVL、.OVY などの拡張子ファイルも感染対象になる場合がある。

古典的なものとしては、.COM、.EXE などの実行可能プログラムの先頭部を強引にウィルスコードで上書き（部分置換）し、実行時に他の実行可能プログラムを探して感染するもの（上書き感染型・部分置換感染型・特殊な直接感染型、これは上書き時にオリジナルソースコード

を破壊して正常な処理はできなくなる)、またこれではすぐ発見されてしまうので、実行型ファイルに付着して（付着場所はプログラムの先頭や末尾が多かったが両端などバリエーションは多い)、感染したプログラムファイルの実行時にシステム制御を奪い他の実行可能プログラムファイルを探して同様に付着し再感染（自己複製）するタイプ（一般的な直接感染型・付着感染型、これは正常なプログラムの処理を中断してウイルスプログラムを実行後に本来の処理に戻るためユーザは感染に気がつきにくい）がある。

ただこれらの古典的なウィルスは感染したプログラムが実行されるという特定のイベント時以外には被害が生じない他、ファイルの大きさをチェックされれば発見されやすい。このような「非メモリ常駐型」に対して被害を大きくしたものがメモリに常駐して DOS の制御を奪う「メモリ常駐型」のウィルスである。これは感染ファイルの実行によりウイルスプログラムがDOS の作業領域または上位メモリに常駐し（DOS の基本的な割り込み機能に寄生する)、未感染ファイルが実行される度に感染が行われる。このため感染が容易であり感染速度も速い。

ウィルスプログラムがメモリに常駐するには感染プログラムの実行だけではなく、感染ディスクによる起動を用いる場合もあり、後述のシステム領域感染型との複合的なものもあることに注意する必要がある。これらのタイプでは、DOS はウィルスに制御を奪われており、ウイルスの命令が優先され常に PC を制御している状態になる。このため実行中のプログラムやアクセス中のメディアに容易に感染する他、ウイルスが常時システムを監視していることにより感染プログラムの実行・非実行にかかわらずイベントトリガの条件を見たせば発病することになる。またメモリ常駐によりユーザ使用可能のメモリを圧迫するので、処理速度が低下したりする症状が出たりする。現在実行可能プログラムファイル感染型の多くは、このメモリ常駐型である。この仲間にはディレクトリ感染ウィルスといった、DOS の DIR コマンドでオープンすると感染したり、DIR を実行したディレクトリのすべてのファイルに感染したりするものもある。

ウイルスをメモリから排除するためには PC の電源を OFF にする必要がある。ウォームブート（[Ctrl]+[Alt]+[Delete]キーによる再起動）では、メモリから排除できないタイプもあるからである。しかしながら PC 内部に常に通電しているメモリやペリフェラル類や、フラッシュメモリが増加してきた今日、この電源 OFF という手段でさえ最終的な排除方法にはならなくなっていることには注意する必要がある。これは後述のシステム領域感染型でも同様である。

（B）システム領域感染型：

ディスク中の MBR、パーティションテーブル、論理ドライブのブートセクタなどのシステム領域に感染するタイプ（ユーザに対しては不可視の領域であるため、発見は難しい)。PC の起動時には必ずここにアクセスするため、PC は自動的に感染状態で起動することになる。起動後ウィルスはメモリに常駐してディスク（HDD、FD ともに）を監視しているので、未感染ディスクにアクセスすればそのシステム領域に感染する。

最も多いのは「ブートセクター感染型ウィルス」といわれるものである。HDD、FD はともにすべての論理ドライブにはブートセクター(フォーマット情報や書き込まれたデータの情報、また DOS システムをロードするためのブートプログラムが置かれている）を持っている。注意しなければならないことは正常にフォーマットされたディスク（HDD、FD ともに）なら、どんなものでもそのブートセクタにはブートプログラムが保存されているため、DOS システムファイルがある起動ディスク（フォーマット時にシステムを転送した FD、sys コマンドを用いシステムを転送するか format 時にコマンドに/s オプションを付けたもの）以外のデータ

しか保存していない FD であっても、実行型プログラムファイルであるブートプログラムはウィルス感染の可能性があるということである。システム領域感染型ウイルスはフォーマット済みであればどんなフロッピーディスクにでも感染することができる。

PC の起動 HDD がブートセクター感染型ウィルスに感染していれば起動ディスクでもデータディスクでも FD を挿入すれば感染するし、逆に感染した起動ディスクで FDD から起動すれば PC 本体の HDD に感染することになる。さらに誤って起動ディスクでもないデータディスクを FDD に残して起動した場合、「Non-system Disk or Disk Error」というメッセージが表示されるが、これは上述のブートプログラムが実行されたためであり、FD が感染していればもはや PC 本体のハードディスクに感染した可能性が高いのである。このようなことは不特定多数のユーザが利用する大学の PC 室などでは日常的に発生するであろう。

この他「マスターブートレコード感染型ウィルス」は、HDD の最初の物理セクタには MBR（マスターブートレコード）とパーティションテーブルがあり、MBR にはマスターブートプログラムという実行型のプログラムファイルがあるがこれに感染する。この感染の仕方はブートセクター感染型ウィルスの場合とまったく同じと考えてよい（フロッピーディスクではブートセクターにこのウィルスが感染する）。

いずれもシステム領域感染型では DOS の起動メカニズムのためにシステムファイルに先んじてウイルスがメモリにロードされ、DOS の割込み制御を完全に奪うことになる点では先のメモリ常駐型の実行可能プログラムファイル感染型と同じである。また対処実務ではシステム領域感染型と実行可能プログラムファイル感染型の分類（感染場所の分類）よりは、DOS の割込み制御を奪いメモリに常駐して感染したりトリガを待つか、またはユーザの実行により感染するかという分類（メモリ常駐／非常駐の分類）の方が有効である。たとえばシステム領域感染型ウイルスは、コンピュータの電源を切るまでメモリに常駐する点ではメモリ常駐型の実行可能プログラムファイル感染型と同じである（前述のようにそれだけでは済まなくなりつつある点も同じ）。

システム領域感染型ウイルスはシステム領域をウイルスプログラムで上書きする際にディスクのシステム領域（ブートセクタやパーティションテーブル）の情報を他の場所へ移動させる。したがって通常の起動プロセスに先んじてウイルスがメモリにロードされ、ウィルスプログラム実行後に、移動先の場所にシステム領域情報を参照に行く。このため DOS 環境ならば一見正常に起動したように見えるのであるが、WindowsNT では NTFS に FAT として上書きしたりすることになるので NTFS は破壊されるという被害が生じることがある（もはや感染しないが破壊はこまる、OS/2 の HPFS でも同様のことが起こる可能性がある）。 さらに近年は「複合感染型」のウィルスとしてファイルと MBR（またはブートセクター）の両方に感染する事例も出てきている。

（2） 経済学部 PC 室の管理とウィルス

実際にネットワーク接続された PC 室設備を管理した場合、以上の事項を理解していても難しい問題が数多く生起する。たとえばネットワーク経由のダウンロードを不可とする（ローカルの HDD もサーバのホームディレクトリも使わせない）、FDD などリムーバブルメディアを使用不可にする、といった方法をとった場合、事実上、講義や演習は不可能であろう（Web ブラウザはアクティブコンテンツを不可にするぐらいは可能）。またウィルス問題は PC 室管理から見れば一部の憂慮事項に過ぎない。部局では問題全体を外患・内憂・自滅という 3 種類に分類してその問題点を検討してきた。

事実、PC 室における管理問題を列挙した場合、「外患」（ネットワーク経由の侵入・破壊、侵入犯による盗被害や物理的破壊）、「内憂」（ウィルス感染メディアの持ち込み、不謹慎データの交換・蓄積、不注意による機器設備の破損・破壊）はもちろんのこと、実は「自滅」（ハードの欠陥・耐久性不足や OS、デバイスドライバ、ソフトの不完全性による稼働率低下）の問題が最大の難関であり、事実、管理時間の大半はこの自滅回避に費やされた。

また、中規模 LAN を組みやすいことや、ネットワークを介してのローカル HDD の回復策が容易であったこと、またウィルス問題も含めてセキュリティ的にも平成 6 年時点で WindowsNT によるサーバ・クライアントですべてシステムを構成し、またシャットダウン権限はユーザには渡したくなかったが、この時点では MS-DOS および Windows3.1 上での講義・演習希望が極めて根強かったことからローカル PC の HDD に FAT 領域と DOS 環境を残さざるをえず、またこのことが予想通りの問題を引き起こした。また WindowsNT にも対応したワクチンソフトが平成 9 年まで無かったため、導入も見合わせていた。

学生ユーザは DOS 環境下で頻雑にリブートを繰り返すため、感染 FD（データ FD の場合も同様）を挿入したままリブートすることによりシステム領域感染型のウィルスが PC 本体に感染する可能性はあるであろうが、毎月 MBR と FAT 領域は Format の上ネットワークを介して完全に再生するため伝染の可能性はそれほど無いと見込んでいた。しかし実態はそれを上回っており、平成 9 年になり修論、卒論作成の時期に調子の良い PC を求めて感染 FD を携えさまよう学生達によると考えられるが、わずかの期間で故障中の PC を除いて多数台が FAT、NTFS 領域ともにウィルスに感染することになった。

NTFS 側の破壊はなかったものの除去が容易ではないタイプであり、また駆除作業の終わった PC 室に再び感染 FD を持ち込もうとする学生への対応、自宅 PC への対応指導、さらに駆除作業中に悪運（？）強く感染したまま故障していた PC が復帰後新たな感染源となったり、症状の軽さの割にはもぐらたたきを絵で書くような大変な騒ぎになった。

結局のところ PC 室の使い勝手を悪くするような方針は取れないため、駆除作業を通してその御利益を確認したワクチンソフトを学部全体で導入し、控えめではあるがウィルス対策の無い PC を部局内では皆無にするという水際防御をまず計り、ついでサーバにある程度ネットワークを通過するファイルも監視できるサーバ専用のワクチンソフトを導入することにした。この点に関しては PC 室および事務室とともに、ほぼ全教官の協力による共同ライセンス購入により、教官室の PC にも同時にワクチンソフトを導入することができた。

教訓的なものになるが、痛感したのは以下の点である。個人用の PC でのウィルス対策とは大きく異なっていると思われる。

- 講義・演習の時間割に影響を与えないために、100 台程度の PC は学部内部の人力のみで 1 ～ 2 晩以内に直ちに回復できるような手段を用意しておくべきである（当 PC 室では全 PC の HDD を MBR も含めすべて清掃した後、FD 1 ～ 3 枚程度で WindowsNT または FreeUNIX により、ネットワークを介して同時に復旧できる準備がしてあった）。
- クリーンなブートディスクやテストのためのスタンドアロン環境を常に用意しておく（いざというときに、どれがクリーンなのか感染の可能性があるか慌てないため、平成 6 年頃はプリインストールモデルでも PC1 台 1 台に MS-DOS のディスケットが付属していたので、未使用起動ディスクが多数あって助かった）。
- PC1 台 1 台の詳細な記録を日頃用意しておく（故障と感染の時期のずれなどをチェックし、「もぐら」を発生させないため）。
- ワクチンソフトのメーカ、またパターンファイルのバージョンによってウィルス警告が出

たり出なかったりすることがあり、ワクチンソフトも完全ではない。比較可能な環境やワクチンソフトを複数用意しておく。

- 100～200台のPCへのワクチンソフトの導入は面倒であり、大学ではそれぞれの管理者に導入をまかせがちであるが、部局が先導して一挙に導入した方が後々のトラブルは回避できる。全体管理者の覚悟が必要である。

以上

参考資料

コンピュータウィルス（一般的なセキュリティを含む）に関するインターネット上のWWWサイトとしては以下のようなものがある。

情報処理振興事業協会(通産省特別認可法人) http://www.ipa.go.jp/SECURITY/index-j.html
ICSA (正式には National Computer Security Association) http://www.icsa.net/
CSI（Computer Security Institute）http://www.gocsi.com/

ワクチンソフトメーカのホームページもウィルスの説明に多くのページを割いている。
TRENDMICRO社（製品：ウィルスバスター）http://www.trendmicro.co.jp/（日本法人）
SYMANTEC. Japan社（製品： Norton AntiVirus）http://www.symantec.co.jp/sarcj/index.html
ネットワーク・アソシエイツ社(旧マカフィー、製品：VirusScan) http://www.nai.com/japan/
コンピュータ･アソシエイツ社（製品：Cheyenne AntiVirus）http://www.caj.co.jp/
同、CAアンチウィルステクニカルセンター http://www.caj.co.jp/avc/avc.htm
EliaShim社 "ViruSafe" Virus Center http://www.eliashim.com/index.html
DataFellows社 http://www.datafellows.com/vir-info/
Dr Solomon's Software社 http://www.drsolomon.com/home/home.cfm
（前記のネットワーク・アソシエイツ・グループの一社になっている。）

また、Nifty-serve に「ウイルス対策フォーラム（FVIRUS）」があるが、インターネットのWWWではフォーラムにはアクセスできない。会員へのサービスのみ。